US Army Corps
of Engineers

CENTRAL SECURITY OFFICER (cSO) MANUAL

Electronic Signature System

Version 2.0

June 30, 1996

CEFMS

Corps of Engineers Financial Management System

FOREWORD

The CEFMS central security officer (cSO) capability is limited to Government employees. In addition to required local training, a designated cSO must read and understand this document before receipt of a cSO smartcard (token). Refer to Appendix A for the signature requirement acknowledging that you have read and understand the cSO's responsibilities.

CENTRAL SECURITY OFFICER (cSO) MANUAL

TABLE OF CONTENTS

CENTRAL SECURITY OFFICER (cSO) MANUAL

TABLE OF CONTENTS (CONT.)

CENTRAL SECURITY OFFICER (cSO) MANUAL

TABLE OF CONTENTS (CONT.)

PAGE

CENTRAL SECURITY OFFICER (cSO) MANUAL

TABLE OF CONTENTS (CONT.)

TABLE OF CONTENTS (CONT.)

CENTRAL SECURITY OFFICER (cSO) MANUAL

TABLE OF CONTENTS (CONT.)

PAGE

LIST OF APPENDICES

1.0 GENERAL

1.1 Purpose.

The purpose of this document is to provide the information necessary to procure, install, configure, secure and operate a Central Key Translation Center (KTC). This document delineates the hardware and operating system used by the KTC and the initial installation and configuration requirements for those components. The operator or user interface to the KTC is presented in detail. Error messages and troubleshooting information are also provided.

1.2 Government Compliances.

Guidance in the design and development of the KTC was obtained from the following standards:

[ANSIX9.17] ANSIX9.17-1985, Financial Institution Key Management (Wholesale), American Banker's Association, Approved April 4, 1985, Reaffirmed 1991.

[FIPS46-2] FIPS PUB 46-2, Data Encryption Standard (DES), US DOC/NIST, Reaffirmed December 30, 1993.

[FIPS112] FIPS PUB 112, Password Usage, US DOC/NIST, May 30, 1985.

[FIPS113] FIPS PUB 113, Computer Data Authentication, US DOC/NIST, May 30, 1985.

[FIPS140-1] FIPS PUB 140-1, Security Requirements for Cryptographic Modules, US DOC/NIST, January 11, 1994.

[FIPS171] FIPS PUB 171, Key Management Using ANSI X9.17, US DOC/NIST, April 27, 1992.

[FIPS180] FIPS PUB 180, Secure Hash Standard (SHS), US DOC/NIST, May 11, 1993. (Superseded by [FIPS180-1]).

[FIPS180-1] FIPS PUB 180-1, Secure Hash Standard (SHS), US DOC/NIST, April 17, 1995.

[FIPS181] FIPS PUB 181, Automated Password Generator (APG), US DOC/NIST, October 1993.

[GAO] Comptroller General of the United States, Comptroller General Decision 71 COMP.GEN.109 (1991), General Accounting Office, 13 December 1991.

The identified standards specify the security requirements that are to be satisfied by a cryptographic module used in protecting unclassified information. The security requirements cover areas related to the secure design, implementation, and use of a cryptographic module. These areas include basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility (EMI/EMC), self testing, and design engineering. The totality of the KTC components, the hardware, operating system, cryptographic modules, and application software provide complete key translation and key management capabilities as defined in the referenced publications.

Direct guidance was provided by the National Institute of Standards and Technology (NIST) and the Government Accounting Office (GAO).

1.3 Operational Design Theory.

1.3.1 The Electronic Signature Process.

An Electronic Signature, or Message Authentication Code (MAC), is a cryptographic checksum calculated by a cryptographic algorithm, based on the Digital Encryption Standard, which resides and executes on a cryptographic module. A cryptographic algorithm must be implemented in firmware residing on a cryptographic module. A cryptographic module is a set of hardware, firmware, and/or software that implements cryptographic algorithms and logic. The information that must be supplied to the cryptographic module so that a MAC can be generated is:

- A secret key belonging to the person signing or MACing the data. This person is the user.
- A secret key belonging to the person allowing the user to electronically sign data. This person is the Security Administrator (SA).
- The data to be MACed.

The secret keys are resident on each SA and user smartcard and in the smartcard database at each KTC. A smartcard (also referred to as "token") is a similar to a credit card but contains a complete computer resident in chip form on the smartcard. The signing process generates a MAC and an encryption key. Please note that the data is not encrypted. The encryption key is used in the verification process and is not an encrypted form of the data. At any point in time, the MAC may be verified. The verification process ensures that none of the data associated with the MAC has changed. The verification process also requires the secret keys of an SA and user. The SA and user that request to verify a MAC do not have access to the secret keys of the SA and user which generated the MAC. This is where key translation comes into the Electronic Signature process. The keys of the SA and user that were used to generate the MAC plus the keys of the SA and user wishing to verify the MAC along with the original encryption key must be sent to the KTC. If the information received by the KTC is valid, the KTC will generate a verification key based upon the received information and send the verification key back to the SA and user wishing to verify the MAC. The process of generating a verification key is *key translation*. The verification key, along with the secret keys of the SA and user wishing to verify the

MAC and the data are input to the cryptographic algorithm which results in the generation of another MAC. If this new MAC and the original MAC are identical the data has not changed. Different MACs indicate that the data has changed and the verification fails.

In addition to providing key translation services, the KTC provides the capabilities to:

- Create User Smartcards
- Create SA Smartcards
- Create District Security Officer (dSO) Smartcards
- Create Central Security Officer (cSO) Smartcards
- Transmit key information between KTCs electronically and on magnetic media

All of the identified capabilities of the KTC provide a complete Key Management System as defined by the referenced standards.

1.3.2 Types of cSO Smartcards.

There are three types of cSO smartcards:

1. Master - these are new card types with KD_{COMM}, KK_{COMM}, and KK_{CMS} keys.

2. Regular - these have the same KD_{COMM} and KK_{COMM} as the corresponding currently logged cSO cards, but with a new KK_{CMS}.

3. Backup - these are identical to the cSO cards currently logged, with the exception of new PINs and User IDs.

1.3.3 The Key Translation Usage.

When any large organization uses Electronic Signature, the number of key translations will be a significant load on the KTC. In operation, many people will be MACing and verifying MACs throughout the work day. Consideration must be given to the following:

- the expected steady or average rate of translate key requests
- the time periods and load for peak translate key requests
- physically disbursed users and computing equipment

Significant numbers of users can be expected to use the Electronic Signature system in the course of daily work. Peak loads will occur when an organization wide function, such as time reporting, must be accomplished within a relatively small time period. The KTC must be on-line 24 hours a day and must be able to handle peak loads significantly higher than average loads.

1.3.4 **The Design Solution.**

The KTC has been implemented using an event driven, multi-process design. The KTC consists of the following processes:

- Master Resource and Scheduling Control (MSRC)
- Request Translate Key Services (RTKS)
- Cryptographic Module Driver (CMD)
- Card Activator (VATOR)
- Remote KTC Communicator (NAGGER)
- KTC Logger (TKLOGD)
- User Interface (TKUI)

A detailed description of those processes is beyond the scope of this document. However, an overview of the functioning of the processes working together is required for an operator to be able to successfully analyze system problems.

All KTC processes use the arrival or sending of a UNIX Inter-Process Communication (IPC) message to control execution flow within the KTC software system. The RTKS process opens network communication points called sockets and listens on those sockets for connection requests for translate key services made by Electronic Signature functions performing verification functions. A translate key request can be made from any device connected to the same Wide Area Network (WAN) as the KTC. When RTKS detects a connection request, RTKS forks a child process to handle the connection request and goes back to listening for other connection requests. The child RTKS completes the connection, receives the data for the translate keys request, and then posts the request and associated data to a message box being listened to by MSRC. If MSRC has no messages in its mailbox, MSRC "sleeps" until a message is detected. When MSRC detects a message, MSRC wakes up and processes all messages in the message box before again going to "sleep". Upon detecting a message in its message box, or queue, MSRC dequeues the message and determines if one of the CMD processes is not busy and can handle the request. If a CMD is not available, MSRC dynamically queues the message in a local memory queue and continues processing on the MSRC message queue. If a CMD is available, MSRC posts the message to that CMDs message queue, marks that CMD as busy and continues processing on the MSRC message queue. The CMD detects the message, wakes up, dequeues the message, performs the translate key operation, and posts the result in the MSRC message queue and continues "sleeping" on its message queue. MSRC dequeues the CMD message, posts the message to the child RTKS process that originally received the request, frees the CMD, and if messages are queued in the local buffer, dequeues the next request and sends that request to the CMD that just finished processing a request. The RTKS child process detects the message in its message queue, wakes up, dequeues the message, transmits the message back through the socket to the originator, closes the socket, and then commits suicide.

If a connection cannot be established with a specific KTC, the electronic signature system automatically tries the other KTC. As can be seen, the process is complicated, but results in efficient and timely processing of translate keys requests.

1.4 KTC Hardware Requirements.

Each KTC requires an on-line or in use system and a complete set of backup hardware. The KTC hardware is described below:

An Intel 80486 PC style computer running at least 33MHz, with:

a. an AT bus, with 8 8 bit slots available after installation of SVGAcard, disk controller card, network card, and serial/parallel card

b. a motherboard with the following capabilities:

   1. 256K of fast cache (20 - 25 nanosecond)
   2. American Megatrends BIOS with standard CMOS, Advanced CMOS, and Advanced Chipset setup capabilities
   3. Symphony Chipset
   4. RAM expandability to 64 Megabytes using 4 Megabyte SIMMs
   5. CPU upgradeability, for example, should be able to change CPU from 486-33 to 486-66 or to Pentium without removing or swapping motherboard

c. room for 2 full height 5.25 hard drives, 2 floppy drives, a tape drive, and CD-ROM drive

d. 32 Megabytes of 70 nanosecond RAM

e. a Super VGA Video card that is compatible with SCO Open Desk Top (which is UNIX 3.2.4), such as an Orchid Prodesigner IIs or Trident 8900 SVGA card

f. a Super VGA Monitor, non-interlaced, .28, or better, dot pitch

g. an Adaptec 1542b or 1542c SCSI Device Controller

h. 2 Seagate ST41200N 1.2 Gigabyte SCSI Hard drives

i. a 3COM 3c503 Ethernet Card

j. a 2 GigaByte SCSI DAT Tape Drive

k. a SCSI CD-ROM drive

l. 8 Electronic Signature printed circuit board cryptographic modules

The KTCs that are delivered and installed consist of the components delineated above in a twin tower configuration. The main tower contains the mother board and a bus expansion card. The bus expansion card provides and additional 8 bus slots to the 7 bus slots provided by the mother board. A cable runs from the bus expansion card to the second tower and connects to another bus expansion card plugged into a motherboard which is just a bus backplane. A SCSI bus cable connects the main tower and the second tower. The second tower also houses the SCSI CD-ROM drive and the SCSI tape backup unit. The main tower houses the 3.5" and 5.25" floppy drives and the two Seagate ST41200N hard disk drives. There is room in the second tower for adding two full height devices.

Substitution of any component or a hardware configuration will result in an inoperable KTC. The KTC has been designed to achieve a high throughput, and that throughput, 50,000 requests per hour, with the components delineated above. The KTC software makes use of specific special capabilities of the identified hardware components and firmware.

1.5 KTC Operating System Requirement.

The KTCs come installed with the Santa Cruz Operation (SCO) Open Desktop (ODT) version 2.0 operating system. SCO ODT is SCO UNIX V/386 version 3.2 release 4. ODT comes with a full C language development system and support for ETHERNET TCP/IP network operations. It is important to note that SCO ODT is a trusted system and has been certified to meet the C2 class of "trust" as defined by the DOD "Trusted Computer System Evaluation Criteria", also known as the "Orange Book". It is also important to note that SCO ODT is fully POSIX compliant. With its extensive communications capabilities and compliance with international and government standards, SCO UNIX also supports interoperability with other systems. Its 32-bit, multi-threaded, multi-tasking, multi-user kernel with virtual memory provides the capabilities necessary for implementing the KTC software design.

1.6 Central Security Officer (cSO) Security Procedures.

Although smartcards are not considered "classified information", and both Processing Centers (CPC and WPC) are designated Unclassified, Sensitive (US2), the security procedures required for cSO smartcard holders are in compliance with the requirements established by the National Institute of Standards and Technology (NIST) and the General Accounting Office (GAO) for safeguarding electronic signature cards.

The KTCs for the Corps of Engineers are located at the Western Processing Center and the Central Processing Center. Each site has a primary active system and a backup. These systems are used for Key Management and Key Translation. The system is managed under the rules of "split knowledge and dual control". All actions related to system operation (other than backups and SCO operating system

software administration) will require a cSO1 and a cSO2 person, each with their own card and PIN (password). All new cSOs should receive local training (as provided in Appendix C) from current cSOs before assuming responsibility as a cSO.

1.6.1 Receiving a cSO Smartcard.

The cSO smartcards and PINs are issued by the primary cSOs; one will issue the card and the other the PIN envelope. Examine the PIN envelope carefully for tampering. If it is okay, sign the front of the envelope (before opening) acknowledging "I have inspected this envelope and can attest that this envelope has not been tampered with prior to my signature." The front of the PIN envelope contains your smartcard serial number and card type. Open the envelope and give the signed top portion to the issuing cSO. The bottom portion contains your PIN. **MEMORIZE THE PIN AND DESTROY THE BOTTOM PORTION OF THE ENVELOPE IN SUCH A MANNER TO ASSURE THE PIN IS NOT READABLE, E.G., BY SHREDDING OR BURNING.** Do not write your PIN down. Memorize it! Loss of a cSO card **AND** PIN will result in a recall and recreation of **ALL** production cSO, dSO, SA, and user cards for the entire Corps of Engineers. The entire data base would have to be rebuilt and all processing would be suspended while new cards and PINs were issued.

1.6.1.1 Storing cSO Smartcards.

A GSA approved container (safe) for storage of classified material is used for storage of cSO cards within the computer room. When a card is not in use, put it in a tamper evident envelope, seal the envelope, and sign your name over the seal on the back of the envelope. Date the envelope and list the contents. The envelope should be serially numbered and tamper evident. Unused envelopes should be stored in a locked container. The cSO1s will be given the combination to drawer/safe one (1) and will store their card (in a tamper-evident signed envelope) in that drawer/safe. The cSO2s will be given the combination to drawer/safe two (2) and store their card (in a tamper-evident signed envelope) in that drawer/safe. The combinations of each drawer/safe is known only by the people required to have access. The combinations of the drawers/safes will be changed annually or whenever there is a change in personnel. Any items/cards removed from or placed into the safe must be recorded on the Safe Log Sheet. A sample log sheet and instructions are provided in Appendix B of this document. A cSO card **will never** leave the work area (computer room).

1.6.1.2 Replacing cSO Smartcards.

Electronic Signature System (ESS) users will have only one smartcard. If a new card is needed for any reason (non-functional, damaged, lost, etc.), report it immediately to a primary cSO. Your old card must first be deactivated by the primary cSOs and reported to the appropriate officials.

1.6.1.3 Unlock a cSO Smartcard.

A cSO smartcard becomes locked after three consecutive failed attempts to enter a PIN. Use the menu option to unlock the smartcard. If it can not be unlocked, the card must be regenerated.

1.6.2 Processing Smartcard Order Requests.

a. The primary duty of a cSO is filling customer smartcard order requests. The rules of "**split knowledge and dual control**" apply when receiving and using a cSO card. A cSO1 and cSO2 must always be present for generating smartcards and PINs. Do not leave the KTC equipment in the middle of a process. If one of the cSOs must leave the area, both cSOs should terminate processing. If both cSO1 and cSO2 must leave the area, close out the function and ensure that the cSO cards are returned to the appropriate drawer/safe.

b. A dSO list will be maintained of all authorized dSOs. The dSOs for each site will be designated to the regional centers by memorandum signed by the Commander. This memorandum will include the dSO type (dSO1 or dSO2), name, phone number, address, and dSO designation (primary or backup). Any changes to the dSO list must also be by memorandum to the regional centers.

The central security officers at the regional centers will not issue a dSO card to anyone who is not on the list (resulting from the memorandum). Card requests and mailing of cards and PINs will only be made to dSOs on the list.

1.6.3 Receiving and Initializing Tokens.

The Request for Electronic Signature (Smartcard Initialization) Form, provided in Appendix D, will be required for dSOs to request any new cards. The cSOs should complete columns b&c, sign and date the form, keep original on file and return a copy to the dSOs. This will serve as a log of all tokens in the ESS. In addition, the electronic request screen in CEFMS should be used to send signed requests to the KTC.

1.6.4 Distribution of Initialized Tokens and PIN Envelopes.

At a minimum, the following procedures should be followed to distribute initialized token and PIN envelopes.

a. The cSO should jointly determine that each token has a corresponding PIN envelope which will be sent, and vice versa.

b. Tokens and PIN envelopes are to be sent in separate mailings, each of which are doubly wrapped in tamper-evident envelopes suitable for sending classified mail; each layer is sealed, and the name and address of both the addressee and sender are written on the outside of each layer. User PIN envelopes should only be mailed to dSO2. SA PIN envelopes should only be mailed to dSO1. User tokens should be mailed to dSO1 and SA tokens mailed to dSO2.

c. Non-cSOs can handle and mail tokens and PIN envelopes, while they are sealed in the envelopes prepared by the cSOs.

d. The cSOs should send the token package of user cards to dSO1; the token package of SA cards to dSO2; then await an acknowledgement of receipt before distributing the second package (on a different day, to a different dSO). The PIN envelopes for SAs should be mailed to dSO1 and PIN envelopes for users should be mailed to dSO2. The receipt of these packages by the dSOs should be followed by a signed acknowledgement to the cSOs.

e. If a package of PIN envelopes is lost, all tokens should be returned to the cSO for reinitialization. If a package of tokens is lost, all PIN envelopes should be destroyed by shredding or burning.

1.6.5 Security of the Smartcard and PIN.

Memorize your PIN and destroy it immediately. **DO NOT** write it down (especially on the smartcard) or share with others.

a. When your card is not in use, store in a tamper-evident envelope, sign the envelope on the seal and return to the proper drawer/safe. Record the return on the Safe Log Sheet (sample provided with instructions in Appendix B).

b. If you retire, transfer, or leave the organization, you must notify the primary cSO and return your smartcard to them for deactivation. Your signed acknowledgement form will be returned to you to be destroyed.

1.6.5.1 Security Violations.

Loss of a smartcard or compromise of a PIN is a serious security issue. You are responsible for both.

a. If your PIN is revealed to someone else or you suspect it has been compromised, contact a primary cSO immediately.

b. If your smartcard is lost/stolen, contact a primary cSO immediately.

c. If you retrieve your smartcard envelope from the safe and it appears it has been tampered with, do not open it; immediately notify your primary.

d. If you find the KTC in an active process and unattended, attempt to log off of the procedure and report it to a primary cSO.

e. If you find a smartcard, return it to a primary cSO.

1.6.5.2 Loss of cSO Smartcard and/or PIN Compromise.

Loss of a cSO card and/or PIN compromise is a very serious security violation! All smartcards for the Corps of Engineers will have to be deactivated and reissued if this type of violation occurs. The following procedures must be followed for a cSO violation.

a. Contact CEFMS project office for assistance.

b. CEFMS must be deactivated as soon as the violation is reported.

c. New cSO cards must be generated.

d. A machine backup including all CEFMS program files and production databases must be generated for the day before the date the card was lost. These tapes must be maintained for seven years.

e. All smartcards must be deactivated and new cards issued to all users, security administrators and district security officers.

f. All CEFMS data must be resigned. Master signing cards will be created for signing of data and only used for this purpose. After the resigning, they will be inactivated and destroyed.

g. A machine backup including all CEFMS program files and production databases must be generated on the day before the date of the resigning. These tapes must be maintained for seven years.

h. CEFMS Disbursing Officers must complete the following procedures:

1. Reconcile disbursing officers' accounts to Treasury reports for checks issued for the period from the lost card date to the resigning date. Document that the SF1219 and SF1220 data has been reconciled. Assure all disbursements are reconcile in accordance with AR 37-1, paragraph 28-8d.

2. Validate all commitments, obligations, receiving reports that occurred during the period from the lost card date to the resigning date using acceptable statistical sampling methods Guidance for statistical sampling for the joint review of unliquidated obligations, AR 37-1, paragraph 28-14f, may be used. Document the procedures followed and the transactions validated.

3. The Disbursing Officer must sign a statement that all transactions reviewed are valid. The signed statement and backup documentation should be maintained for seven years.

i. Due to the severity of the cSO smartcard violation, it is extremely important that security procedures for storage of cSO cards are followed. **The cSO smartcards and PINS should never be removed from the secure area of the Key Translation Center.**

1.6.6 Deactivation of cSO Smartcards.

1.6.6.1 Inoperable cSO.

If a cSO is unable to perform cSO duties for an extended period of time, that cSO's token should be deactivated by two other cSOs, and the removal of the cSO's duties should be noted on the list of authorized cSO names and phone numbers maintained by the Corps.

1.6.6.2 Routine Termination of Responsibilities.

If a cSO retires, transfers or leaves the organization, his cSO token should be deactivated by two other cSOs and the removal of the cSO's duties should be noted on the list of authorized cSO names and phone numbers maintained by the Corps.

1.6.7 Transfer of Key Database.

If one KTC copies the key database to magnetic media and delivers it by mail to the other KTC to synchronize the databases, the magnetic media should be packaged in a manner consistent with the procedures addressed in paragraph 1.6.4(b) of this document.

2.0 KEY TRANSLATION CENTER INSTALLATION

Section 2.0 provides detailed information to install and configure the KTC.

*****This Section provides an outline for future documentation.*****

2.1 Security Considerations

2.2 Site Selection

2.3 Hardware Installation and Configuration

2.3.1 SCSI Bus Parameters

2.3.2 SCSI Device IDs

2.3.3 Formatting SCSI Hard Disk Drives

2.3.3.1 Formatting Disk Drives with the Adaptec 1542B SCSI Controller

2.3.3.2 Formatting Disk Drives with the Adaptec 1542C SCSI Controller

2.3.4 Bus Interconnection Between Cabinets

2.3.5 Electronic Signature Cryptographic Module Configuration

2.4 SCO Open Desktop Installation and Configuration

2.4.1 SCO Installation Procedure

2.4.1.1 Disk Drives, Partitions, and File Systems

2.4.2 SC0 UNIX Configuration

2.4.2.1 UNIX Kernel Parameters

2.4.2.2 Creating Emergency BOOT and ROOT Floppies

3.0 KEY TRANSLATION CENTER (KTC) OPERATIONS

This section explains the various aspects of using the Key Translation Center (KTC), including required security procedures, starting the software, using the software and configuring the system, and making backups and restorations of certain pertinent files in the system. The Corps of Engineers has four (4) KTC systems with only two in operation at one time (one at each processing center) The two systems at the Western Processing Center are designated TK1 and TK3 and the two systems at the Central Processing Center are designated TK2 and TK4. Primary active systems are TK3 and TK4 with TK1 and TK2 used for backup and parts as needed. The KTC systems at the processing centers are used for Key Management and Key Translation. The system is managed under the rules of "split knowledge....dual control".

3.1 KTC Security Procedures.

Until a complete risk assessment and system accreditation is completed, the KTC will have a designation of Unclassified-Sensitive two (US2). Operation, handling of KTC material, and procedures for delivery of orders will be accomplished as though the operators are handling classified material.

3.1.1 Physical Security of the KTC Equipment and Accessories.

- The KTC hardware is physically maintained in the locked restricted access computer room.
- The Central Security Officer (cSO) and backup cSO cards are locked in a two drawer safe, cSO1 cards in one drawer, cSO2 cards in the other drawer. Each drawer has a separate combination lock known only to the security officers (1 or 2) using that drawer. The safe is located in the computer room. Opening, closing and use of material in the safe is recorded on a Safe Log Sheet (see Appendix B).

- Blank non-keyed cards are stored under lock and key.

- The computer room exterior is constantly monitored by video camera and recorded.

- Key Translation i.e. generating "user cards", always requires a cSO1 and cSO2.

- Orders that are filled and waiting (2nd day) shipment are locked in the safe.

3.1.2 Additional Security for System Operation

- Each appointed cSO is briefed at the time of appointment on the responsibilities of that assignment and the security required. Briefings are given using the KTC Security Briefing Checklist (Appendix C).

- UNIX operating system (SCO) root password is known only by the UNIX system administrator and his/her backup. The root password is recorded, placed ina sealed envelope and stored in the locked safe.

- Only government employees will be designated as cSO's.

- Tamperproof envelopes are printed on an impact printer with the ribbon removed to lessen the possibility of seeing the passwords on the exterior of the envelope.

- A security check will be completed at the end of normal day shift. This will include a review of the Safe Log Sheet, assuring the safe drawers are closed and locked, and assuring the drawe indicators show "CLOSED".

3.2 Starting the Key Translation Center Operations Software.

The Key Translation Center is started by following these steps:

A Security Officer will log in to the KTC as user "root".

Change from the root directory to the homedirectory for the user "trankey". In default installations of the Key Translation software, this directory is "/usr2/trankey". The command "cd ~trankey" at the UNIX system prompt puts the system in the proper directory.

Start the Master Scheduler process by typing "msrc" at the UNIX prompt.

Security Officer smartcards must be logged into each cryptographic module installed in the system via that adapter's smartcard reader. The system prompts for each card to be placed in the numbered smartcard reader, and for the PIN associated with that card to be typed in. Ninety seconds ae allowed by the system for each cryptographic module to be initialized. If this time limit expire before both Central Security Officer smartcards have been logged, the Key Translation Cente software shuts down automatically.

When all cryptographic modules have been brought up in this manner, the Operator Interfae process begins. The Key Translation Center is operational at this point, and the *Operator Interface Main Screen* is visible. Once the *Operator Interface Main Screen* is visible, cSO2 may safely remove his card from the last smartcard reader.

3.3 The Operator Interface.

The Operator Interface is responsible for providing a consistent interface between the Security Officers and the Key Translation Center. The Operator interface uses pop-up windows and menus for all user/system interaction. In most windows or menus, pressing the ESC key takes the user to the previous menu or window. The computer's arrow keys are used to move the highlight bar when applicable.

The Operator Interface Main Screen is displayed when the Operator Interface begins. This screen is composed of five parts: the *title bar*, the *navigation bar*, the *main interface menu*, the *error message area*, and the *owner notice bar*.

The *title bar* is used merely to display the title of the system, "Key Translation Center".

The *navigation bar* displays at any given time the current position within the Operator Interface. For example, upon startup, this bar displays "KTC Main Menu". If the Security Officers move into another menu, the title in the navigation bar changes to reflect the new position.

The *main interface menu* is discussed fully in Section 3.4.

The *error message area* displays the current system error message, along with the time the error occurred. This area is cleared at any time by pressing the "v" key while in the *KTC Main Menu.*

The *owner notice bar* displays the owner of this Key Translation Center, the U.S. Army Corps of Engineers.

3.4 The Key Translation Center Main Menu.

The *Key Translation Center Main Menu* is shown in Figure 3.1 and provides the following 7 options: 1) User Database Maintenance, 2) Smartcard Management, 3) Configure System, 4) Network Monitor, 5) Do Total System Backup, 6) Refresh KTC Display and 7) Shutdown Translate Keys Server.

This menu, like most other menus in the system, is operated in one of two ways. The up- and down-arrow keys are used to navigate the magenta highlight bar to the intended option, and the ENTER key is pressed to select the option. For more experienced users, pressing the keyboard key corresponding to the highlighted blue letter on the intended option automatically moves the highlighted bar to that option and selects it.

3.4.1 User Database Maintenance Menu.

When the Security Officers select the first option from the *KTC Main Menu*, "User Database Maintenance", the *User Database Maintenance Menu* appears in a separate window. This menu is composed of four options; 1) Query User Database (2) View User Database, (3) Export user data base to tape, and. (4) Import User data base from tape. The *User Database Maintenance Menu* is operated

in the same way as the *KTC Main Menu*. Pressing the ESC key at this point closes the window containing this menu and returns control to the *KTC Main Menu*.

Query User Database option allows the Security Officers to query the user database for a particular user or group of users. When this option is selected, the *Query User Information Window* opens, and control is given to it. This window is used to select a subset of users from the whole CORPS for viewing. The up- and down-arrow keys are used to move the black cursor to the field (or fields) upon which to query.

The Security Officers must type in the values for the fields on which to match the query. Entering a percent (%) sign at either the beginning or end of the field value causes zero or more characters to be matched for that value in the query. For example, entering "FRED%" in the "First name" value field finds all people whose names begin with "FRED". Entering "%ES" finds all people whose names end with "ES". Entering "%R%" finds all people whose first names contain the letter "R". Pressing the F3 key executes the search, and pressing the ESC key cancels the query request, closes the *Query User Information Window*, and returns control to the *User Database Maintenance Menu*.

If only one match is found for the given query criteria, the *User Information Window* opens (see Section 3.4.1.4) with the information for the requested user shown. If more than one match is found, *User Query Multiple Choice Window* opens. Each entry in this window is composed of a user's organization code, last name, first name, and identification number. The up- and down- arrow keys are used to navigate this window. Pressing Enter opens the *User Information Window* for that user (see Section 3.4.1.4), and pressing the ESC key cancels the query, removes the window, and returns control to the *User Database Maintenance Menu*.

View User Database

Selecting this option from the *User Database Maintenance Menu* allows the Security Officers to view the KTC user database. Entries in this database are listed in a scrollable window, with the users' organization code, last name, first name, and identification number shown. Entries are shown in the order that they were added to the database. Use the up- and down- arrow keys to navigate this window, and press Enter on the desired record to select it for viewing. When a user is selected for viewing, the *User Information Window* is opened, and that user's information is displayed there. Pressing the ESC key here removes this window and gives control back to the *User Database Maintenance Menu*. This window displays all the available information about a given user. The following information is shown: first name, last name, identification number, home phone, work phone, organization code, organization address, organization city, state, and zip code, card number, and the active status of the user's smartcard. An "X" between the square brackets in the "Active" field indicates that the card shown in the "Card number" field is active for this user. Pressing the ESC key removes this window and gives control back to the window or menu that opened it.

Export user data base to tape

The *Export user data base to tape* option gives Security Officers the capability to write the user file to tape. Prior to selecting this option a tape should be inserted into the tape drive on the KTC. When this option is selected the *Export Progress* window is displayed. The *Export Progress* window displays a horizontal moving bar that indicates the percentage of the user file that has been written to tape. When 100% of the user file has been written to tape a prompt will be displayed indicating that a key should be depressed to continue. When a key is depressed control is returned to the *Smartcard Management Menu*. It is recommended that the user database be written to tape daily and that the most recent 30 tapes be kept on hand.

Import user data base from tape

The *Import user data base from tape* option gives Security Officers the capability to restore a user file from tape. Prior to selecting this option a tape containing a user file should be inserted into the tape drive on the KTC. When this option is selected the *Import Progress* window is displayed. The *Import Progress* window displays a horizontal moving bar that indicates the percentage of the user file that has been read from tape and written to disk. When 100% of the card file has been processed a prompt will be displayed indicating that a key should be depressed to continue. When a key is depressed control is returned to the *Smartcard Management Menu*. After this option has completed, the KTC must be shut down and re-started for the new file to be used. This should be done immediately after the import completes.

3.4.2 Smartcard Management Menu.

The *Smartcard Management Menu* is opened when the Security Officers selects the "Smartcard Management" option from the *KTC Main Menu*. This menu is operated in the same way as the KTC Main Menu and has twelve different options:

1) Create a new user card
2) Create a new security administrator card
3) Create a new security officer card
4) Unlock a user smartcard
5) View smartcard database
6) Check for smartcard orders
7) Print dummy envelope
8) Export card file to tape
9) Import card file from tape
10) Export card file to file
11) Import card file from file
12) Spoil cards.

Create New Card Window is opened whenever a new smartcard is to be created by the Key Translation Center. This process **always** requires a cSO1 and cSO2. The window is used as a general output/prompt window for the card creation process. During this process, the following things occur:

a. The KTC finds an available smartcard reader to be used for the card creation. If the system is under a heavy load, this could take several seconds.

b. If there is a smartcard already in the available reader, the cSOs are prompted to remove that card.

c. The cSOs are prompted to login again with their cSO cards on the card reader selected for the card creation process.

d. The cSOs are prompted to insert the new smartcard into the available reader.

e. A new pronounceable UID and PIN are generated by the KTC for the card to be created. This process occasionally takes several seconds to complete.

f. The new card is generated by the KTC. This takes up to one minute per card.

g. A secure envelope is printed with the card serial number, card type, and PIN printed on it.

h. The Security Officers are prompted to remove the new card.

i. At this point, if User, System Administrator, or District Security Officer Cards are being created, the cSOs are prompted to insert another new card to be created. Another card may be created or the Escape key may be depressed to terminate the card creation process which will cause the *Smartcard Management Menu* to be redisplayed. When creating cSO cards, the cSOs must login with their cSO cards for each cSO card created.

At any time during the process of creating a new card, up to the time when the new card is inserted into the smartcard reader, the Security Officers can press the ESC key to cancel the operation. If the operation is canceled by the Security Officers, control returns to the *Smartcard Management Menu*.

3.4.2.1 Create A New User Card.

This option is chosen when the Security Officers need to generate a new user smartcard. Choosing this option opens the *Create New Card* Window. and requires all items above in the *Create New Card* Window.

3.4.2.2 Create A New Security Administrator Card.

This option is chosen when the Security Officers needs to generate a new Security Administrator (SA) card. Choosing this option opens the *Create New Card* Window. and requires all items above in *Create New Card* Window.

3.4.2.3 Create A New Security Officer Card.

This option is chosen when the Security Officers need to generate a new security officer card. Choosing this option opens the *Create Security Officer Card Menu*. This menu has 8 options:

1) Create a district SO1 card
2) Create a district SO2 card
3) Create a central SO1 card
4) Create a central SO2 card.
5) Create a backup cSO1 card
6) Create a backup cSO2 card
7) Create a master cSO1 card
8) Create a master cSO2 card

The up- and down-arrow keys are used to navigate this menu. Pressing the Enter key selects the highlighted option and pressing the ESC key gives control back to the *KTC Main Menu*.

- **Create A District Security Officer 1 (dSO1) Card** option is chosen when the Security Officers need to generate a new district security officer 1 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the *Create New Card* Window.

- **Create A District Security Officer 2 (dSO2) Card** option is chosen when the Security Officers need to generate a new district security officer 1 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the *Create New Card* Window.

- **Create A Central Security Officer 1 (cSO1) Card** option is chosen when the Security Officers need to generate a new central security officer 1 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the *Create New Card* Window. This function will create a cSO1 card with different encryption keys than the currently logged on cSO1 but will have the same communication keys. This will allow secure communications between KTC sites, such as CPC and WPC.

- **Create A Central Security Officer 2 (cSO2) Card** option is chosen when the Security Officers need to generate a new central security officer 2 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the *Create New Card*

Window. This function will create a cSO2 card with different encryption keys than the currently logged on cSO2 but will have the same communication keys. This will allow secure communications between KTC sites, such as CPC and WPC.

- **Create A Backup Security Officer 1 (bcSO1) Card** option is chosen when the Security Officers need to generate a backup central security officer 1 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the*Create New Card* Window. This function will create a cSO1 card with all encryption keys identical to the currently logged on cSO1. bcSO1 cards should be used only at the site where created.

- **Create A Backup Central Security Officer 2 (bcSO2) Card** option is chosen when the Security Officers need to generate a backup central security officer 2 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the*Create New Card* Window. This function will create a cSO2 card with all encryption keys identical to the currently logged on cSO2. bcSO2 cards should be used only at the site where created.

- **Create A Master Central Security Officer 1 (cSO1) Card** option is chosen when the Security Officers need to generate a master central security officer 1 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the*Create New Card* Window. This function will generate a cSO1 card with all new keys. This function should only be used to create a cSO1 card for new electronic signature implementations outside of the Corps or to create a new cSO1 card for the Corps when existing cSO1 card(s) become compromised.

- **Create A Master Central Security Officer 2 (cSO2) Card** option is chosen when the Security Officers need to generate a master central security officer 2 card. Choosing this option opens the *Create New Card* Window. and requires all the items above in the*Create New Card* Window. This function will generate a cSO2 card with all new keys. This function should only be used to create a cSO2 card for new electronic signature implementations outside of the Corps or to create a new cSO2 card for the Corps when existing cSO2 card(s) become compromised.

3.4.2.4 Unlock a User Smartcard.

This menu option allows the Security Officers to unlock a locked user card. A user card becomes locked when a user removes his card from his smartcard reader before properly exiting CEFMS. If a user reboots his machine or turns off his machine before properly exiting CEFMS, his card becomes locked. Locked cards can be returned to the KTC (either WPC or CPC where the card was originally generated) to be unlocked. Since the time that this function was incorporated on the KTC, software has been written to allow users to unlock their own cards at their own site. For that reason, this function will be little used.

When this option is chosen by the Security Officers, the*Unlock User Smartcard Window* is opened, and the following steps occur:

1. The KTC finds an available smartcard reader for unlocking the card.

2. If there is a card already in the reader, the Security Officers are prompted to remove that card from the reader.

3. The Security Officers are prompted to insert the user's smartcard into the reader.

4. The user card is unlocked. This usually takes about five seconds, depending on the system key translation load.

5. Once the card is unlocked, the Security Officers are prompted to remove that card from the reader.

6. cSO2 is prompted to place his card in the reader and type in his PIN.

7. When the *Unlock User Smartcard Window* disappears, the cSO2 should remove his smartcard from the reader.

3.4.2.5 <u>View Smartcard Database</u>.

This option allows the Security Officers to view the contents of the smartcard database. When this option is selected, the *View Smartcard Database Window* is opened, and the card information is shown in a scrollable window. The information is sorted by smartcard UID by default. Using the left- and right-arrow keys, the Security Officers change the field on which the sort is performed. The cards are shown sorted by any one of the following fields: UID, serial number, CEFMS identification number, cryptoperiod expiration date, card activation date, or card creation date. Any time the sort criteria changes, the cards are resorted, and the window is reset to display the cards in their new order. Pressing the ESC key removes this window and gives control back to the*Smartcard Management Menu*.

The Security Officers use the up- and down-arrow keys to select different cards for displaying. Pressing the Enter key opens the *View SmartCard Database* Window. The F1 key is used to search for a specific card depending on the column highlighted. For instance, if the serial number column is highlighted, pressing F1 will cause a search window to be opened at the bottom of active window. The cSOs can then enter the serial number to search for and then press the enter key. If the card with the desired serial number is in the database, the active database window will change to display that record. If the card does not exist no change will occur in the active window.

The following information is displayed in this window: smartcard UID, smartcard serial number, CEFMS user id, smartcard status, smartcard type, smartcard cryptoperiod expiration date, smartcard

activation date and smartcard creation date. Information displayed is extracted from the “keydb” file. The keydb file contains the following fields:

UID = 8 character smartcard specific user id. Sometimes referred to as the MAC UID. This field is displayed in the first column of the *View Smartcard Database* Window.

CardNum = smartcard serial number, stored as a long. This field is displayed in the second column of the *View Smartcard Database* Window.

KK = smartcard encrypting key stored as an unsigned character string. This field is not displayed.

CardType = smartcard stored in a character, 1 = user card, 2 = SA card, 3 = dSO1 card, 4 = dSO2 card, 5 = cSO1 card, 6 = cSO2, 7 = bcSO1 card and 8 = bcSO2 card. . This field is displayed in column 5 of the *View Smartcard Database* Window. However, card types are displayed as follows: “US” for user cards, “SA” for SA cards and “SO” for a dSO1 and dSO2 card. CSO cards are not displayed.

Status = status of smartcard stored in a character variable where 1 = ACTIVE, 2 = INACTIVE, 3 = ARCHIVE, 4 = LOST and 5 = SPOILED. This field is displayed column 4 of the *View Smartcard Database* Window. However, card status is displayed as follows: “ACT” = ACTIVE, “INACT” = INACTIVE, “ARCHV” = ARCHIVED, “LOST” = LOST and “SPOIL” = SPOILED.

Group = privilege group number stored as a long, will always be 0 for CEFMS. This field is not displayed.

Crypto = crypto period expiration date, stored in an unsigned long in the form YYMMDD. This field is displayed in column 6 of the *View Smartcard Database* Window.

CreateDate = date smartcard was created, stored in an unsigned long in the form YYMMDD. This field is displayed in column 8 of the *View Smartcard Database* Window.

ActivateDate = date smartcard was activated, stored in an unsigned long in the form YYMMDD. This field is displayed in column 7 of the *View Smartcard Database* Window.

LostDate = date smartcard was lost, stored in a long in the form YYMMDD. This field is not displayed.

CreatLoc = location where smartcard was created, stored in a character string. This field is not displayed.

ActivateLoc = location where smartcard was activated, stored in a character string. This field is not displayed.

CreateSO1 = UID of cSO1 that created the card, stored in a character string. This field is not displayed.

CreateSO2 = UID of cSO2 that created the card, stored in a character string. This field is not displayed.

ActSO1 = UID of the dSO1 that activated the card, stored in a character string. This field is not displayed.

ActSO2 = UID of the dSO2 that activated the card, stored in a character string. This field is not displayed.

IDNo = application specific id (CEFMS Id no) of the person the card has been issued to. This field is displayed in column 3 of the *View Smartcard Database* Window.

Pressing the ESC key removes this window and gives control back to the *View Smartcard Database Window*.

3.4.2.6 Check for Smartcard Orders.

When new smartcard orders come in from a CORPS district, this menu option is used to view them. Choosing this option opens the *Pending Smartcard Orders Window*. Smartcard order requests are checked throughout the day. This scrollable window shows the following information: location requesting new smartcards, number of user, SA, and dSO cards requested, smartcard UIDs of the two dSOs making the card request, and the date the new cards were requested. This information is transferred to the "Request for Electronic Signature Cards" form.

The up- and down- arrow keys are used to move the highlight bar to different card orders. Pressing the space bar marks an order with an asterisk, indicating to the system that the Security Officers have received and filled the order. Pressing the ESC key closes the *Pending Smartcard Orders Window*, deletes the asterisk-marked card orders, and returns control to the *Smartcard Management Menu*.

3.4.2.7 Print Dummy Envelope.

The *Print Dummy Envelope* option gives Security Officers the capability to print a secure envelope for proper vertical alignment of the envelopes in the printer. X's are printed on the locations on the envelope where valid data would be printed. If the X's do not appear in the proper location, move the envelopes up and down a small amount. Select the *Print Dummy Envelope* option again. Repeat the process if further adjustment is necessary. Note that ribbons **SHOULD NOT** be used in the printer.

3.4.2.8 Export Card File to Tape

The *Export Card File to Tape* option gives Security Officers the capability to store the user keydb, encrypted and signed with the KD_{com} to tape. Prior to selecting this option a tape should be placed in the tape drive on the KTC. When this option is selected the *Export Progress* window is displayed. The *Export Progress* window displays a horizontal moving bar that indicates the percentage of the card file that has been encrypted and written to tape. When 100% of the card file has been encrypted and written to tape a prompt will be displayed indicating that a key should be depressed to continue. When a key is depressed the control is returned to the *Smartcard Management Menu*. It is recommended that the card database be written to tape daily and that the most recent 30 tapes be kept off site. The Security Officers should then export the user data base file to tape.
Whenever a card file is exported, the Security Officers should then immediately export the user database file and label both tapes to indicate that they are a pair that, should the need arise, be imported together.

3.4.2.9 Import Card File from Tape.

The *Import Card File from Tape* option gives Security Officers the capability to restore a card file from tape that has been written to tape with the *Export Card File to Tape* option. Prior to selecting this option a tape containing a valid exported card file should be placed in the tape drive on the KTC. When this option is selected the *Import Progress* window is displayed. The *Import Progress* window displays a horizontal moving bar that indicates the percentage of the card file that has been read, decrypted and read from disk. When 100% of the card file has been processed a prompt will be displayed indicating that a key should be depressed to continue. When a key is depressed the control is returned to the *Smartcard Management Menu*. The user data base file on the corresponding tape should then be imported. After this option has completed, the KTC must be shut down and re-started for the new card file and user file to be used by the KTC. This should be done immediately after the import completes.

3.4.2.10 Export Card File to File.

The *Export Card File to File* option gives Security Officers the capability to store the user keydb, encrypted and signed with the KD_{com} to card file, suitable for transmission to their KTC sites electronically with tools such as FTP. Each card file record is read, encrypted under the communication keys and written to a disk file specified by the "exportfile" entry in the "tkui" section of the "tk.ini" configuration file. When this option is selected the *Export Progress* window is displayed and functions as described in 3.4.2.8. After the Export Card File to File has completed, the export file can then be transmitted to other KTC sites where it must be imported before use. The user data base file must be transmitted at the same time as the exported card file.

3.4.2.11 **Import Card File from File**.

The *Import Card File from File* option gives Security Officers the capability to convert an exported card file for use by the KTC. Prior to selecting this option the Security Officers must make sure that the file to be imported has the name and path specified by the "importfile" entry in the "tkui" section of the "tk.ini" configuration file. When this option is selected the *Import Progress* window is displayed and functions as described 3.4.2.9. After this option has completed, the KTC must be shut down and re-started for the new card file to be used. This should be done immediately after the import completes.

3.4.2.12 **Spoil Cards**.

The *Spoil Cards* option gives the capability to change the status of a smartcard from INACTIVE to SPOILED. This will allow a card to be re-created immediately. If, during the creation of a card, the PIN envelope tears, or the PIN is otherwise compromised, the card cannot be sent to site. To re-create that card it must be spoiled.

3.4.3 **Configure System Menu**.

The *Configure System Menu* gives the Security Officers the capability to reconfigure various aspects of the Key Translation Center. Choosing the "Configure System" option from the Main Menu opens a window containing the *Configure System Menu*. Configuration options are listed by process in the Key Translation Center. These options are: 1) Master scheduler configuration, 2) Network transmitter configuration, 3) User interface configuration, 4) System logger configuration, 5) Cryptographic Module configuration, 6) Card manager configuration, and 7) Remote communicator configuration. These selections are explained in Sections 3.4.3.1 through 3.4.3.7.

Selecting one of the options from the *Configure System Menu* brings up a second menu, pertaining to the particular process being configured. Selecting one of the options from any of these secondary menus opens the *Configure System Parameter Window*. This window always shows the parameter being configured in it's title line. This window also shows the current value for the given system parameter, and prompts for a new value for the parameter. Pressing the ESC key closes this window without making any changes to the system parameter; typing a new value for the parameter and pressing Enter changes the system parameter and closes the window. If the Security Officer presses Enter without entering a new value for the parameter, the window closes and the parameter is not changed. Any time this window closes, control is given back to the menu which called it.

3.4.3.1 **Master Scheduler Configuration Menu**.

The *Master Scheduler Configuration Menu* is used to configure the various tunable parameters of the Master Scheduler process. These parameters are: 1) base translate keys path, 2) number of cryptographic modules installed, 3) system log file path, 4) primary translate keys host name, 5) secondary translate keys host name, 6) network service name, 7) network protocol, 8) backup

message queue base size, 9) backup message queue increment size, and 10) the master scheduler nice value. These options are discussed in Sections 3.4.3.1.1 through 3.4.3.1.10.

The up- and down-arrow keys are used to move the highlight bar to the desired selection. Pressing the Enter key chooses that selection and opens the *Configure System Parameter Window*, discussed in Section 3.4.3. Pressing the ESC key closes the *Master Scheduler Configuration Menu* and returns control to the *Configure System Menu*.

3.4.3.1.1 Base Translate Keys Path.

This is the default path where certain system files used by the Key Translation Center are stored. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.1.2 Number of Cryptographic Modules Installed.

This is the number of cryptographic module boards installed in the Key Translation Center. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.1.3 System Log File Path.

This is the path to the directory where the system log files are to be stored. The value for this parameter in a default installation is "/usr2/trankey", the "trankey" user's home directory. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on how to use this window.

3.4.3.1.4 Primary Translate Keys Host Name.

This is the network node name of the Key Translation Center machine . Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.1.5 Secondary Translate Keys Host Name.

This is the network node name of the Secondary Key Translation Center machine. All Key Translation Centers have a backup system. This is the machine that the remote communicator communicates with when sending requests for card activations. Choosing this option opens the *Configure System Parameter Window.* See Section 3.4.3 for an explanation on using this window.

3.4.3.1.6 **Network Service Name**.

This is the name of the network service (found in the /etc/services file) that the Key Translation Center uses to advertise its offerings to the CEFMS system nodes. The default value for this parameter is "tk_services". Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.1.7 **Network Protocol**.

This is the type of protocol the Key Translation Center uses for its network communications. The default value for this parameter is "tcp", and should not be changed at this time, because CEFMS will be running on a TCP/IP based network.

3.4.3.1.8 **Backup Message Queue Base Size**.

When all cryptographic modules in the Key Translation Center are busy, the Master Scheduler process buffers key translation records in an internal queue. This parameter is the base size (in records) for this queue, and its default value is 100. If the system load is very large (100 to 200 requests queued (see Section 3.4.4 on the Network Monitor) at peak times), the Security Officers may wish to increase this number to improve system performance. If the Key Translation Center has a relatively light load during peak times, this number can be decreased to give the system more memory. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.1.9 **Backup Message Queue Increment Size**.

Read Section 3.4.3.1.8 before reading this paragraph. When the system load is heavy, there are times when the backup message queue becomes full. At that time, it becomes necessary for the Master Scheduler Process to allocate more space for the queue to use. This parameter is used to set the number of records by which the queue should be incremented. The default value for this parameter is 50 records. If the system is very busy, this parameter can be increased to maximize system performance. For the best performance, this parameter should be incremented/decremented by at least 50 records each time it is modified. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.1.10 **Master Scheduler Nice Value**.

This parameter is used to set the UNIX Master Scheduler process nice value. This parameter tells the UNIX system at what priority to run a process. The smaller a nice value is, the higher the priority of that process. Great care should be exercised when changing this parameter, because it could adversely affect the performance of the Key Translation Center. Only experienced UNIX system administrators should change this parameter.

This parameter has a default value of -13. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

For a more complete explanation of process nice values, see Section 3.4

3.4.3.2 Network Transmitter Configuration Menu.

The *Network Transmitter Configuration Menu* is used to configure the various tunable parameters of the Network Transmitter process. This is the process that is responsible for receiving all requests from different CEFMS sites. The tunable parameters are: 1) path to executable, 2) card request file name, and 3) process nice value.

The up- and down-arrow keys are used to move the highlight bar to the desired selection. Pressing the Enter key chooses that selection and opens the *Configure System Parameter Window*, discussed in Section 3.4.3. Pressing the ESC key closes the *Network Transmitter Configuration Menu* and returns control to the *Configure System Menu*.

3.4.3.2.1 Path to Network Transmitter Executable.

This is the home directory where the Network Transmitter executable is stored. The value for this parameter in a default installation is "/usr2/trankey". The name of the executable is "rtks", and should not be included in the path. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.2.2 Card Request File Name.

This is the full path to and name of the file used by the Key Translation Center to hold the information for pending smartcard orders. These orders come on a district basis, and are used when various districts need to order new smartcards. The value for this parameter in a default installation is "/usr2/trankey/card.requests". Choosing this option opens the *Configure System Parameter Window*. See section 3.4.3 on using this window.

3.4.3.2.3 Network Transmitter Nice Value.

This parameter is used to set the UNIX Network Transmitter process nice value. This parameter tells the UNIX system at what priority to run a process. The smaller a nice value is, the higher the priority of that process. Great care should be exercised when changing this parameter, because it could adversely affect the performance of the Key Translation Center. Only experienced UNIX system administrators should change this parameter.

This parameter has a default value of 0. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

For a more complete explanation of process nice values, see Section 3.4.

3.4.3.4 Operator Interface Configuration Menu.

The *Operator Interface Configuration Menu* is used to set the various tunable parameters of the Operator Interface process. This process is responsible for directing all interaction between the Security Officers and the Key Translation Center. The tunable parameters for this process are: 1) path to executable, 2) path to user database file, 3) path to smartcard database file, 4) number of lines on PIN envelopes, 5) line to print PIN on PIN envelope, 6) column to print PIN on PIN envelope, 7) line to print hyph-PIN on PIN envelope, 8) column to print hyph-PIN on PIN envelope, 9) line to print smartcard serial number on PIN envelope, 10) column to print smartcard serial number on PIN envelope, 11) line to print smartcard type on PIN envelope, 12) column to print smartcard type on PIN envelope, 13) printer device name, and 14) operator process nice value.

The up- and down-arrow keys are used to move the highlight bar to the desired selection. Pressing the Enter key chooses that selection and opens the*Configure System Parameter Window,* discussed in Section 3.4.3. Pressing the ESC key closes the*Operator Interface Configuration Menu* and returns control to the *Configure System Menu.*

3.4.3.3.1 Path to Operator Interface Executable.

This is the home directory where the Operator Interface executable is stored. The value for this parameter in a default installation is "/usr2/trankey". The name of the executable is "tkui", and should not be included in the path. Choosing this option opens the*Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.2 Path to User Database File.

This is the directory where the Key Translation Center user database file is stored. This file is called "userdb" and by default is in the "/usr2/trankey" directory. If this entry is changed, the name of the user database file should be the last element of the path. For example, the default value of this parameter is "/usr2/trankey/userdb", where the actual path is "/usr2/trankey" and the file name is "userdb". Choosing this option opens the*Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.3 Path to Smartcard Database File.

This is the directory where the Key Translation Center smartcard database file is stored. This file is called "keydb" and by default is in the "/usr2/trankey" directory. If this entry is changed, the name of the smartcard database file should be the last element of the path. For example, the default value of this parameter is "/usr2/trankey/keydb", where the actual path is "/usr2/trankey" and the file name is "keydb". Choosing this option opens the*Configure System Parameter Window.* See Section 3.4.3 for an explanation on using this window.

3.4.3.3.4 **Number of Lines on PIN Envelopes**.

This parameter holds the number of text lines available on the secure PIN envelopes. The CORPS standard at the time of this writing dictates 33-line (half-page) envelopes. This parameter should be changed if different envelopes are ever used in the Key Translation Center.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.5 **Line to Print PIN on PIN Envelope**.

This parameter holds the value for the line on the secure PIN envelope where the PIN will be printed. The default value for this parameter is 22. If the CORPS standard ever dictates a new kind of secure envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.6 **Column to Print PIN on PIN Envelope**.

This parameter holds the value for the column on the secure PIN envelope where the PIN will be printed. The default value for this parameter is 30. If the CORPS standard ever dictates a new kind of secure envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.7 **Line to Print Hyph-PIN on PIN Envelope**.

This parameter holds the value for the line on the secure PIN envelope where the hyphenated pronounceable PIN will be printed. The default value for this parameter is 23. If the CORPS standard ever dictates a new kind envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.8 Column to Print Hyph-PIN on PIN Envelope.

This parameter holds the value for the column on the secure PIN envelope where the hyphenated pronounceable PIN will be printed. The default value for this parameter is 5. If the CORPS standard ever dictates a new kind of secure envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the Configure System Parameter Window. See Section 3.4.3 for an explanation on how to use this window.

3.4.3.3.9 Line to Print Smartcard Serial Number on PIN Envelope.

This parameter holds the line on the secure PIN envelope where the smartcard serial number will be printed. The default value for this parameter is 14. If the CORPS standard ever dictates a new kind of secure envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.10 Column to Print Smartcard Serial Number on PIN Envelope.

This parameter holds the line on the secure PIN envelope where the smartcard serial number will be printed. The default value for this parameter is 35. If the CORPS standard ever dictates a new kind of secure envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.11 Line to Print Smartcard Type on PIN Envelope.

This parameter holds the line on the secure PIN envelope where the smartcard type (USER, SA, dSO) will be printed. The default value for this parameter is 12. If the CORPS standard ever dictates a new kind of secure envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.12 Column to Print Smartcard Type on PIN Envelope.

This parameter holds the line on the secure PIN envelope where the smartcard type (USER, SA, dSO) will be printed. The default value for this parameter is 5. If the CORPS standard ever dictates a new kind of secure envelope, this parameter may need to be changed. Some experimentation by the Security Officers may be required to get this parameter tuned exactly.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.13 Printer Device Name.

This parameter holds the path and device name for the printer used to print secure envelopes on the Key Translation Center. The default value of this parameter is "/dev/lp0". If it becomes necessary to change this parameter, the Security Officers must be sure to include the full path for this device.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.3.14 Operator Process Nice Value.

This parameter is used to set the UNIX Operator Interface process nice value. This parameter tells the UNIX system at what priority to run a process. The smaller a nice value is, the higher the priority of that process. Great care should be exercised when changing this parameter, because it could adversely affect the performance of the Key Translation Center. Only experienced UNIX system administrators should change this parameter.

This parameter has a default value of 5. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

For a more complete discussion on setting process nice values, see Section 3.4

3.4.3.3.15 Exportfile Value.

This value specifies the path and file to be created when the card file is exported to a file.

3.4.3.3.16 Importfile Value.

This value specifies the path and file to be read when importing the card file.

3.4.3.4 System Logger Configuration Menu.

The *System Logger Configuration Menu* is used to set the various tunable parameters of the System Logger process. This process is responsible for keeping a log of all requests received by the system. The tunable parameters for the System Logger are: 1) path to executable, 2) maximum log buffer size, 3) number of log files to maintain, and 4) process nice value.

The up- and down-arrow keys are used to move the highlight bar to the desired selection. Pressing the Enter key chooses that selection and opens the *Configure System Parameter Window*, discussed in Section 3.4.3. Pressing the ESC key closes the *System Logger Configuration Menu* and returns control to the *Configure System Menu*.

3.4.3.4.1 Path to System Logger Executable.

This is the home directory where the System Logger executable is stored. The value for this parameter in a default installation is "/usr2/trankey". The name of the executable is "tklogd", and should not be included in the path.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.4.2 Maximum Log Buffer Size.

While keeping a log of Key Translation Center events, the System Logger maintains an internal buffer space, so that KTC performance is maximized. This parameter is used to set the size of that buffer, in bytes. If the Center is under a heavy load, this value may be increased for better performance (optimum performance comes if the size of the buffer is a power of 2). If, however, there is a system crash for any reason, the contents of the log file buffer will be lost. For this reason, discretion should be used when increasing the size of this parameter.

This parameter has a default value of 8192. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.4.3 Number of Log Files to Maintain.

This parameter is used to set the number of log files to maintain, in days. These files are created on a daily basis, and the file names take the form "YYMMDD.log". For example, the log file for January 23, 1994 would be named "940123.log". The Security Officers should maintain at least one week's worth of log files.

This parameter has a default value of 7. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.4.4 System Logger Process Nice Value.

This parameter is used to set the UNIX System Logger process nice value. This parameter tells the UNIX system at what priority to run a process. The smaller a nice value is, the higher the priority of that process. Great care should be exercised when changing this parameter, because it could adversely affect the performance of the Key Translation Center. Only experienced UNIX system administrators should change this parameter.

This parameter has a default value of -1. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

For a more complete discussion on setting process nice values, see Section 3.4

3.4.3.5 Cryptographic Module Configuration Menu.

The *Cryptographic Module Configuration Menu* is used to set the various tunable parameters of the Cryptographic Module process. This process is responsible for handling all requests that require the use of a cryptographic module. These include translation of keys, creation of cards, and card activation requests. The tunable parameters for this process are: 1) path to executable, 2) cryptographic module base addresses, and 3) process nice value.

The up- and down-arrow keys are used to move the highlight bar to the desired selection. Pressing the Enter key chooses that selection and opens the *Configure System Parameter Window*, discussed in Section 3.4.3. Pressing the ESC key closes the *Cryptographic Module Configuration Menu* and returns control to the *Configure System Menu*.

3.4.3.5.1 Path to Cryptographic Module Executable.

This is the home directory where the Cryptographic Module executable is stored. The value for this parameter in a default installation is "/usr2/trankey". The name of the executable is "sad", and should not be included in the path.

This parameter has a default value of 5. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.5.2 Cryptographic Module Base Addresses Identification.

These parameters allow the Security Officers to set the base hardware address of each cryptographic module in the Key Translation Center. The Security Officers must consult the manual supplied with the cryptographic module hardware to learn how to set the address. The values for these parameters should always match the values set on the adapter hardware. The Key Translation Center will not work properly if these values are not correctly set.

These parameters have different default values. This option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.5.3 Cryptographic Module Process Nice Value.

This parameter is used to set the UNIX Cryptographic Module process nice value. This parameter tells the UNIX system at what priority to run a process. The smaller a nice value is, the higher the priority of that process. Great care should be exercised when changing this parameter, because it could adversely affect the performance of the Key Translation Center. Only experienced UNIX system administrators should change this parameter.

This parameter has a default value of -12. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

For a more complete discussion on setting process nice values, see Section 3.4

3.4.3.6 Smartcard Manager Configuration Menu.

The Smartcard Manager Configuration Menu is used to set the various tunable parameters of the Smartcard Manager process. This process is responsible for maintaining the database of smartcards. The tunable parameters for this process are: 1) path to executable and 2) process nice value.

The up- and down-arrow keys are used to move the highlight bar to the desired selection. Pressing the Enter key chooses that selection and opens the *Configure System Parameter Window*, discussed in Section 3.4.3. Pressing the ESC key closes the *Smartcard Manager Configuration Menu* and returns control to the *Configure System Menu*.

3.4.3.6.1 Path to Smartcard Manager Executable.

This is the home directory where the Smartcard Manager executable is stored. The value for this parameter in a default installation is "/usr2/trankey". The name of the executable is "vator", and should not be included in the path.

This parameter has a default value of 5. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.6.2 Smartcard Manager Process Nice Value.

This parameter is used to set the UNIX Smartcard Manager process nice value. This parameter tells the UNIX system at what priority to run a process. The smaller a nice value is, the higher the priority of that process. Great care should be exercised when changing this parameter, because it could adversely affect the performance of the Key Translation Center. Only experienced UNIX system administrators should change this parameter.

This parameter has a default value of 0. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.7 Remote KTC Communicator Configuration.

The *Remote KTC Communicator Configuration Menu* is used to set the various tunable parameters of the Remote KTC Communicator process. This process is responsible for alerting the secondary Key Translation Center to all changes in the smartcard database. The tunable parameters for this process are: 1) path to executable, 2) name of request queue file, 3) time to delay between transmissions to secondary machine, and 4) process nice value.

The up- and down-arrow keys are used to move the highlight bar to the desired selection. Pressing the Enter key chooses that selection and opens the *Configure System Parameter Window*, discussed in Section 3.4.3. Pressing the ESC key closes the *Remote KTC Communicator Configuration Menu* and returns control to the *Configure System Menu*.

3.4.3.7.1 Path to Remote KTC Communicator Executable.

This is the home directory where the Remote KTC Communicator executable is stored. The value for this parameter in a default installation is "/usr2/trankey". The name of the executable is "nagger", and should not be included in the path.

Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.7.2 Path to Remote KTC Communicator Request Queue File.

This is the path to the request queue file maintained by the Remote KTC Communicator. This file is used when requests are not acknowledged by the secondary Key Translation Center. The full path and file name should always be specified when changing this parameter.

This parameter has a default value of "/usr2/trankey/rem_requests.que". Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.7.3 Delay Between Remote Communication Connection Requests.

This parameter is used to set the amount of time to delay (in seconds) between requests to the secondary Key Translation Center when it is determined (by the primary Center) that the secondary Center is not responding. For best system performance, especially under heavy loads, this parameter should not be set to less than 900 seconds (15 minutes).

This parameter has a default value of 900. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

3.4.3.7.4 Remote KTC Communicator Nice Value.

This parameter is used to set the UNIX Remote KTC Communicator process nice value. This parameter tells the UNIX system at what priority to run a process. The smaller a nice value is, the higher the priority of that process. Great care should be exercised when changing this parameter, because it could adversely affect the performance of the Key Translation Center. Only experienced UNIX system administrators should change this parameter.

This parameter has a default value of 0. Choosing this option opens the *Configure System Parameter Window*. See Section 3.4.3 for an explanation on using this window.

For a more complete discussion on setting process nice values, see Section 3.4

3.4.4 Network Monitor Screen.

This option, selection from the *KTC Main Menu*, provides the Security Officers with visual feedback on the current state of the Key Translation Center. Visuals are provided for watching board activity, network activity, and system activity.

3.4.4.1 Board Watch.

This window provides a visual interface to the cryptographic module hardware installed in the Key Translation Center. The Security Officers can watch the status of each board in the system, and a total board activity meter.

3.4.4.1.1 Active Boards (Cryptographic Modules).

This window provides a visual representation of the current state of each Cryptographic Module board in the Key Translation Center. Each "block" represents one board in the system. The two-digit numbers above each block designate the number of the board. The board blocks are different colors depending on the state of the board. These colors, and their corresponding meanings, are:

blue - board is inactive, ready for a new request
yellow - board is processing a request
red - board is defective and not in use (may not be completely hardware related. If this occurs, shut down the Key Translation Center, bring down the UNIX system, and restart everything. If the board is still defective, it may need to be replaced)
gray - board is not installed or not in use by the Key Translation Center

3.4.4.1.2 **Total Activity**.

This meter provides visual feedback to the Security Officers on how busy the Key Translation Center is. The meter is a light blue color, and is located in the Total Activity window. If there is nothing visible in this window, no activity is occurring. The meter grows from left to right. When it completely fills the width of the Total Activity Window, the Cryptographic Module boards are being operated at 100% of their capacity.

3.4.4.2 **Request Watch**.

The Request Watch window provides a visual feedback on the current key translation requests going through the Key Translation Center.

3.4.4.2.1 **Address Originating Request**.

This field shows the network node address, in Internet type format, of the machine that made that particular request to the Key Translation Center.

3.4.4.2.2 **In and Out Time of Request**.

These fields show the time received and time dispatched for each key translation request to the Key Translation Center. These times are in the format "HH:MM:SS:TTT", where HH is hours, MM is minutes, SS is seconds, and TTT is thousandths of seconds.

3.4.4.3 **Info Watch**.

The Info Watch window is responsible for displaying values about key translation requests that have been processed by the Key Translation Center. Several different values are shown, including values for errors, number of messages through the system, message load on a per-board basis, and Key Translation Center software up-time.

3.4.4.3.1 **Starting Message Sequence Value**.

This field shows the overall total number of key translation requests received by the Key Translation Center before its last startup.

3.4.4.3.2 **Current Message Sequence Value**.

This field shows the overall total number of key translation requests that the Key Translation Center has received.

3.4.4.3.3 Total Processed Requests.

This field shows the total number of key translation requests (errors are included in this total) that have been processed by the Key Translation Center.

3.4.4.3.4 Elapsed Time.

This field shows the total amount of time (hours, minutes, seconds) that the Key Translation Center software has been running.

3.4.4.3.5 Total Errors.

This field shows the total number of failed key translation requests.

3.4.4.3.6 Board (Cryptographic Module) Request Counters.

These counters show the number of key translation requests processed by each of the cryptographic modules in the Key Translation Center. If there is a gray "N/A" in the counter field, then that particular board is not installed or is not being used.

3.4.5 Do Total System Backup.

When selected, this *KTC Main Menu* option will backup all filesystems on all hard drives to tape in cpio format.

3.4.6 Refresh KTC Displays.

When selected, this *KTC Main Menu* option will clear the screen and re-draw the *KTC Main Menu*. This is useful when the screen becomes cluttered and perturbated from UNIX console error messages.

3.4.7 Shutdown Translate Keys Center.

This option, selectable from the KTC Main Menu, shuts downs the Key Translation Center software. When this option is selected, the console screen clears and all KTC software processed is stopped. Once the UNIX shell prompt is available, the Key Translation Center may be rebooted (using the UNIX "reboot" command) or shut down (using the UNIX "shutdown" command).

3.5 Process Interaction and Nice Value Setting
3.5.1 Translate Keys Center Software Processes and Priorities
3.5.2 Modifying Default Nice Values
3.6 Log Files
3.6.1 Log File Format

3.11.1 Reinitialization of Expired Tokens

When cSO tokens reach the end of their lifetime, one year after issuance, new cSO keys must be generated. This results in the need for the *KKs stored in the user key database to be translated form the old cSO keys to the new ones. The reinitialization procedure follows:

1) Two primary cSOs authenticate themselves to the KTC.
2) The cSOs, using the KTC software, export the user key database to a file. This decrypts the encrypted *KKs using the exclusive-ORed $*KK_{COM}$s, and re-encrypts the *KKs under the exclusive-OR of the cSOs' $*KK_{COM}$s. All of the key records in the database, which include the re-encrypted *KKs, are written to a file on the KTC.
3) The cSOs generate two new "regular" cSO tokens for themselves. These new tokens will have new randomly generated $*KK_{CMS}$ components, but will still contain the same $*KK_{COM}$ and KD_{COM} components as the logged in cSO tokens.
4) The cSOs shutdown the KTC and restart it using their new tokens.
5) The user key database is imported from the file (from step 2 above) and the encrypted *KKs are decrypted using the exclusive-ORed $*KK_{COM}$s and then re-encrypted under the notarized exclusive-OR of the new $*KK_{CMS}$s.

At this point, each user key database's *KKs will be encrypted under the new $*KK_{CMS}$ components at each KTC site, and cSOs will have new tokens. However, the $*KK_{COM}$ and $*KD_{COM}$ values on all cSO tokens at each site must be regenerated, too (due to their expired lifetimes). A utility in the KTC software is provided for cSOs to randomly generate those communication keys and export them to the tokens, replacing the old keys. Before doing so, cSOs should agree upon which KTC site will generate the new communication keys. Once they are generated, they should be securely transmitted to the other KTC site, encrypted under the exclusive-OR of the old $*KK_{COM}$ components. The primary cSOs at the second KTC site then decrypt those new keys and export them to their new tokens. It is critical that the new key components be under the sole control of their proper owner (i.e., the cSO1s should not have access to the cSO2s' new communication key

components and vice versa). Once all of the primary cSOs have tokens with all new key values, then "backup" tokens should be generated for all other cSOs at each KTC site.

APPENDIX A

CSO ACKNOWLEDGEMENT FORM

I certify that I have read and understand my responsibilities as a Central Security Officer (cSO) and that I am a Government employee.

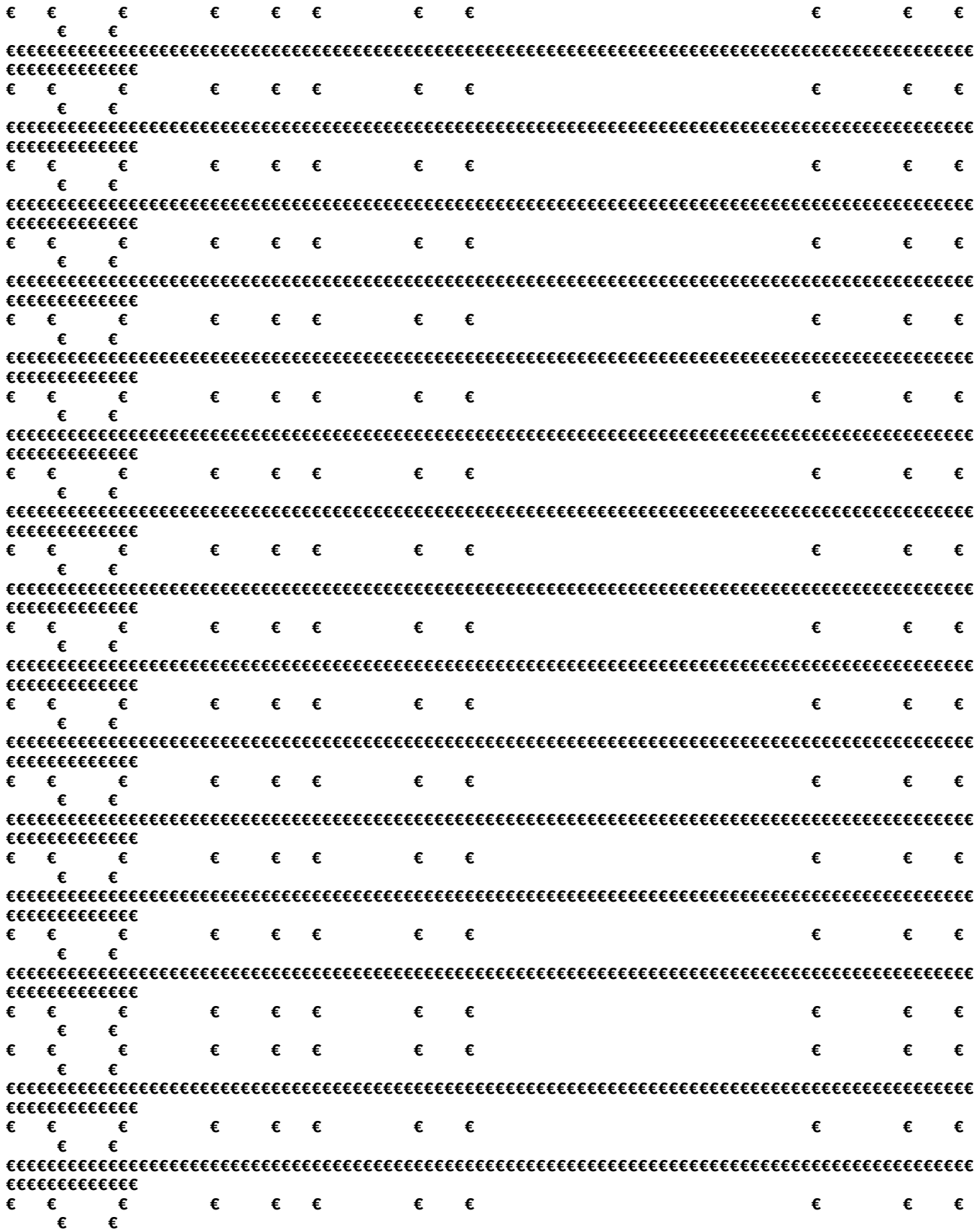
PRINTED OR TYPED NAME	SIGNATURE

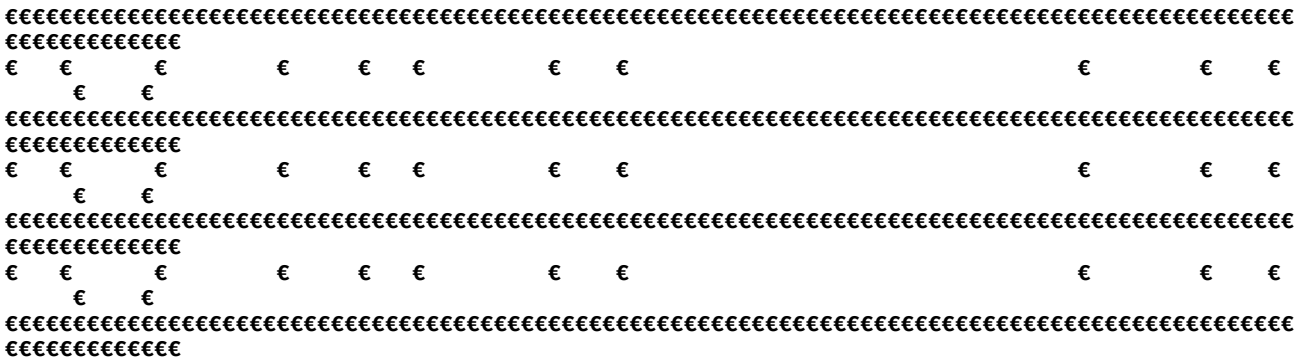
OFFICE SYMBOL	EXTENSION	DATE

APPENDIX B

SAFE LOG SHEET & INSTRUCTIONS

€€
€€€€€€€€€€€€€
€ KEY TRANSLATION CENTER €
€ SAFE LOG SHEET €
€€
€€€€€€€€€€€€€
€MONNH/YEAR €I certify that by my initials below I have opened, removed or inserted material, closed this €
€ €safe, or checked/verified one of these actions in accordance with pertinent agency regulations€
€ €and operating instructions. €
€€
€€€€€€€€€€€€€
€ € € ORDERED BY € ITEMS REMOVED (R) OR INSERTED (I)* € CLOSED BY € CHECKED BY €
€ €
€€
€€
€ € € € € € BY € € € € € €
€ €DRAWER€ € € * €€€€€€€€€€€€€€€€ € € € € €
€DAY€ NO. €INITIALS€ TIME€R/I€INITIALS €TIME€ DESCRIPTION/PURPOSE €INITIALS€TIME€INITIALS€TIME€
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€
€ € € € € € € € € € € € €
€€
€€€€€€€€€€€€€





Instructions for Entries on the Sample Safe Log Sheet

THIS FORM IS DESIGNED FOR ONLY ONE ENTRY PER LINE to assure a detailed audit trail of the activities. The exceptions are if you open the safe/drawer and remove items at that time, OR if you insert items and close/lock the safe/drawer. All other actions must be recorded on a separate line. If open/remove or insert/close do not occur together, they also must be recorded on a separate line.

MONTH/YEAR Numeric month and year for entries contained on this sheet. Format is MM/YY. A new sheet is used for each new month.

DAY Numeric day of month.

SAFE/DRAWER NO Separate safes are labeled Safe No. 1 and Safe No. 2. If a two drawer safe is used, the top drawer is number is No. 1 and the bottom drawer is No. 2.

OPENED BY

INITIALS of person opening safe or drawer. Opening includes using the correct combination to UNLOCK the safe/drawer and turning the OPEN/CLOSED magnetic strip to OPEN.

TIME is local clock time

ITEMS REMOVED (R) OR INSERTED (I)

R/I indicate **R** if items are removed from safe/drawer, or **I** if items are inserted in safe/drawer. If items are removed/inserted at a time other than when the safe/drawer is opened/closed, this requires a new entry on the form.

BY

INITIALS of person inserting or removing items from safe/drawer

TIME is local clock time

DESCRIPTION of items inserted or removed from safe/drawer

CLOSED BY

INITIALS of person closing safe or drawer. Closing is also LOCKING the safe/drawer and turning the magnetic OPEN/CLOSED strip to CLOSED.

TIME is local clock time

CHECKED BY can be done at any time and is required to be done with the normal daily security check. Checking is to assure the drawer(s)/safe is locked and the magnetic OPEN/CLOSED strip indicates CLOSED.

APPENDIX C

CENTRAL SECURITY OFFICER (cSO) BRIEFING

APPENDIX C

Key Translation Center (KTC)
Central Security Officer (cSO) Briefing

GENERAL. Each government employee assigned as a KTC Central Security Officer (cSO) will be given a briefing prior to beginning their assigned duties. Briefings will be given by the primary cSOs. The purpose of the briefing is to assure the assigned cSO understands the functions of the KTC, the relationship between the Electronic Signature System and CEFMS, the principal of "split knowledge and dual control" and completely understands his/her security responsibilities and cSO duties.

EXECUTION. Selection of primary and alternate cSO will be made from available government employees with appropriate background investigation and clearance. The briefing will be given to the employee who then signs the acknowledgment in Appendix A that he/she has received the briefing and understands the responsibilities and duties of a cSO. A copy of the briefing and the signed acknowledgment is given to the cSO. The original is filed in the ISSO's office. If the employee is relieved of cSO duties for any reason, the signed copy is removed from the file and returned to the employee, or destroyed by the ISSO.

a. Initial briefing will include a short overview of the Corps of Engineers Financial Management System (CEFMS) in relation to the Electronic Signature System.

b. Each appointed cSO will receive the "formal" briefing on the security aspects of the system and be required to sign and date the cSO Responsibilities sheet acknowledging understanding and acceptance of responsibilities.

c. All designated cSOs are required to have a Computer Security Awareness briefing (if it has not already been received) within their TASO area.

d. Each person assigned cSO responsibilities is required to attend an annual review/update briefing or training by CEFMS project office.

C-1

cSO BRIEFING

You have been selected to perform the duties of a Central Security Officer (cSO) on the KTC at this Processing Center (CPC or WPC). Although the cards are not considered "classified information", and the center is designated US2, the security procedures you are required observe once you receive your card, are in compliance with the requirements established by the National Institute of Standards and Technology (NIST) and the General Accounting Office (GAO) for safeguarding electronic signature cards.

The KTC's for the Corps of Engineers are located at the Western Processing Center and the Central Processing Center. Each site has a primary active system and a backup. These systems are used for Key Management and Key Translation. The system is managed under the rules of "split knowledge and dual control". All actions related to system operation (other than backups and SCO operating system software administration) will require a cSO1 and a cSO2 person, each with their own card and PIN (password).

RECEIVING YOUR cSO SMARTCARD:

a. You receive your cSO card and PIN from the primary cSOs; one will issue the card and the other the PIN envelope.

b. Examine the PIN envelope carefully for tampering. If it is okay, sign the front of the envelope (before opening) acknowledging "I have inspected this envelope and can attest that this envelope has not been tampered with prior to my signature." The front of the PIN envelope contains your smartcard serial number and card type. Open the envelope and give the signed top portion to the issuing cSO. The bottom portion contains your PIN. **MEMORIZE THE PIN AND DESTROY THE BOTTOM PORTION OF THE ENVELOPE IN SUCH A MANNER TO ASSURE THE PIN IS NOT READABLE, E.G., BY SHREDDING OR BURNING.** Do not write your PIN down. Memorize it! Loss of a cSO card **AND** PIN will result in a recall and recreation of **ALL** production cSO, dSO, SA, and user cards for the entire Corps of Engineers. The entire data base would have to be rebuilt and all processing would be suspended while new cards and PIN's were issued.

c. A GSA approved container (safe) for storage of classified material is used for storage of cSO cards within the computer room. cSO1 individuals will be given the combination to drawer/safe one (1) and store their card (in the signed envelope) in that drawer/safe. cSO2 individuals will be given the combination to drawer/safe 2 (2) and store their card (in the signed envelope) in that drawer/safe. The combinations of each drawer/safe is known only by the people required to have access. The combinations of the drawers/safes will be changed annually or whenever there is a change in personnel. Any items/cards removed from or placed into the safe must be recorded on the KTC Security Safe Check Sheet (NPD Form 380-1 [Temporary]). No cSO card will ever leave the work area (computer room). When you are not using your card and are done with it, you will put it in a tamper-evident envelope, seal the envelope, and sign your name over the seal on the back of the envelope and replace it in the correct safe/drawer.

d. You will have only one smartcard. If you need a new card for any reason (non-functional, damaged, lost, etc.) report it immediately to a primary cSO. Your old card must first be deactivated by the primary cSO's and reported to the appropriate officials.

cSO RESPONSIBILITIES

Processing Smartcard Order Requests. Your primary duty as cSO is filling customer smartcard order requests. The rules of "**split knowledge and dual control**" apply when receiving and using a cSO card. A cSO1 and cSO2 must always be present for generating smartcards and PINs. Do not leave the KTC equipment in the middle of a process. If one of you must leave the area the other must remain but CANNOT CONTINUE processing. If both cSO1 and cSO2 must leave the area, close out the function and insure that the cSO cards are returned to the appropriate drawer/safe.

SECURITY OF THE SMARTCARD AND PIN. Memorize your PIN and destroy it immediately. **DO NOT** write it down (especially on the smart card) or share with others.

a. When your card is not in use, seal in an envelope, sign the envelope on the seal and return to the proper drawer/safe. Record the return on the safe log form.

b. If you retire, transfer, or leave the organization, you must notify the primary cSO's and return your smartcard to them for deactivation. Your signed acknowledgment form will be returned to you or destroyed.

SECURITY VIOLATIONS - WHAT SHOULD YOU REPORT? Loss of a smartcard or compromise of a PIN is a serious security issue. You are responsible for them.

a. If your PIN is revealed to someone else or you suspect it has been compromised, contact a primary cSO immediately.

b. If your smartcard is lost/stolen, contact a primary cSO immediately.

c. If you retrieve your smartcard envelope from the safe and it appears it has been tampered with, do not open it; immediately notify your primary.

d. If you find the KTC in an active process and unattended, attempt to log off of the procedure and report it to a primary cSO.

e. If you find a smartcard return it to a primary cSO.

_____has been designated a cSO1/cSO2 on _____

Printed Name **Date**

MY SIGNATURE BELOW ACKNOWLEDGES THAT I UNDERSTAND THE ABOVE ITEM S AND I HAVE BEEN BRIEFED ON MY DUTIES AND RESPONSIBILITIES AS A cSO. ALSO, I RECEIVED A COPY OF THE BRIEFING MATERIAL FOR MY REFERENCE AND USE. FURTHER, I UNDERSTAND ALL THE SECURITY PROCEDURES AND HAV E QUESTIONED ANY AREAS OF THEM THAT I AM UNCLEAR OF.

_____ _____

Signature **Office Symbol**

APPENDIX D

REQUEST FOR ELECTRONIC SIGNATURE FORM (Smartcard Initialization)

REQUEST FOR ELECTRONIC SIGNATURE FORM
(Smartcard Initialization)

REQUESTING SITE: _____

NAME (dSO1): _____ **Phone No.: ( ) -** _____

MAILING ADDRESS (dSO1): _____

_____

NAME (dSO2): _____ **Phone No.: ( ) -** _____

MAILING ADDRESS (dSO2): _____

_____

CARD REQUESTS:

NO. OF USER CARDS: _____

NO. OF SA CARDS: _____

NO. OF dSO CARDS: _____

SIGNATURES:

dSO1: _____ **dSO2:** _____

a. Card Serial No.	b. Date of Initialization	c. Destination dSO1/dSO2

SIGNATURES:

cSO1: _____ **cSO2:** _____